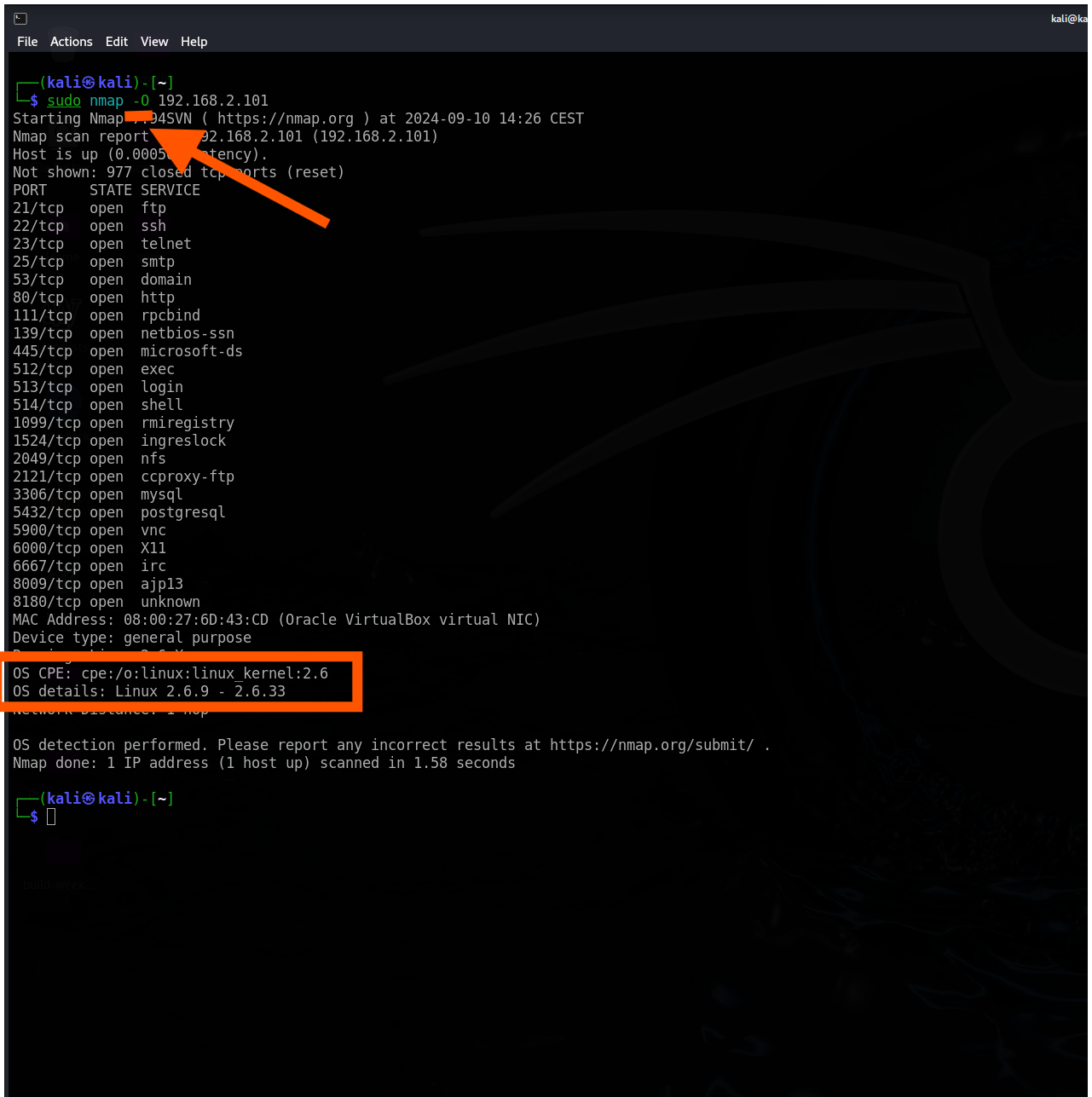


CONSEGNA 10 SETTEMBRE

Sono risalito al tipo di OS usando il comando `sudo nmap -O <IP TARGET METASPLOITABLE >`.



```
(kali@kali)-[~]
$ sudo nmap -O 192.168.2.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 14:26 CEST
Nmap scan report for 192.168.2.101 (192.168.2.101)
Host is up (0.0005s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:6D:43:CD (Oracle VirtualBox virtual NIC)
Device type: general purpose
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds

(kali@kali)-[~]
$
```

SISTEMA OPERATIVO: **LINUX 2.6.9 – 2.6.33**

IP METASPLOITABLE: **192.168.2.101** – IP KALI: 192.168.2.103

Ho ottenuto in output tutte le **versioni** delle porte aperte sulla macchina Metasploitable immettendo il comando **sudo nmap -sV <IP TARGET METASPLOITABLE>**.

```
(kali@kali) - [~]
$ sudo nmap -sV 192.168.2.101

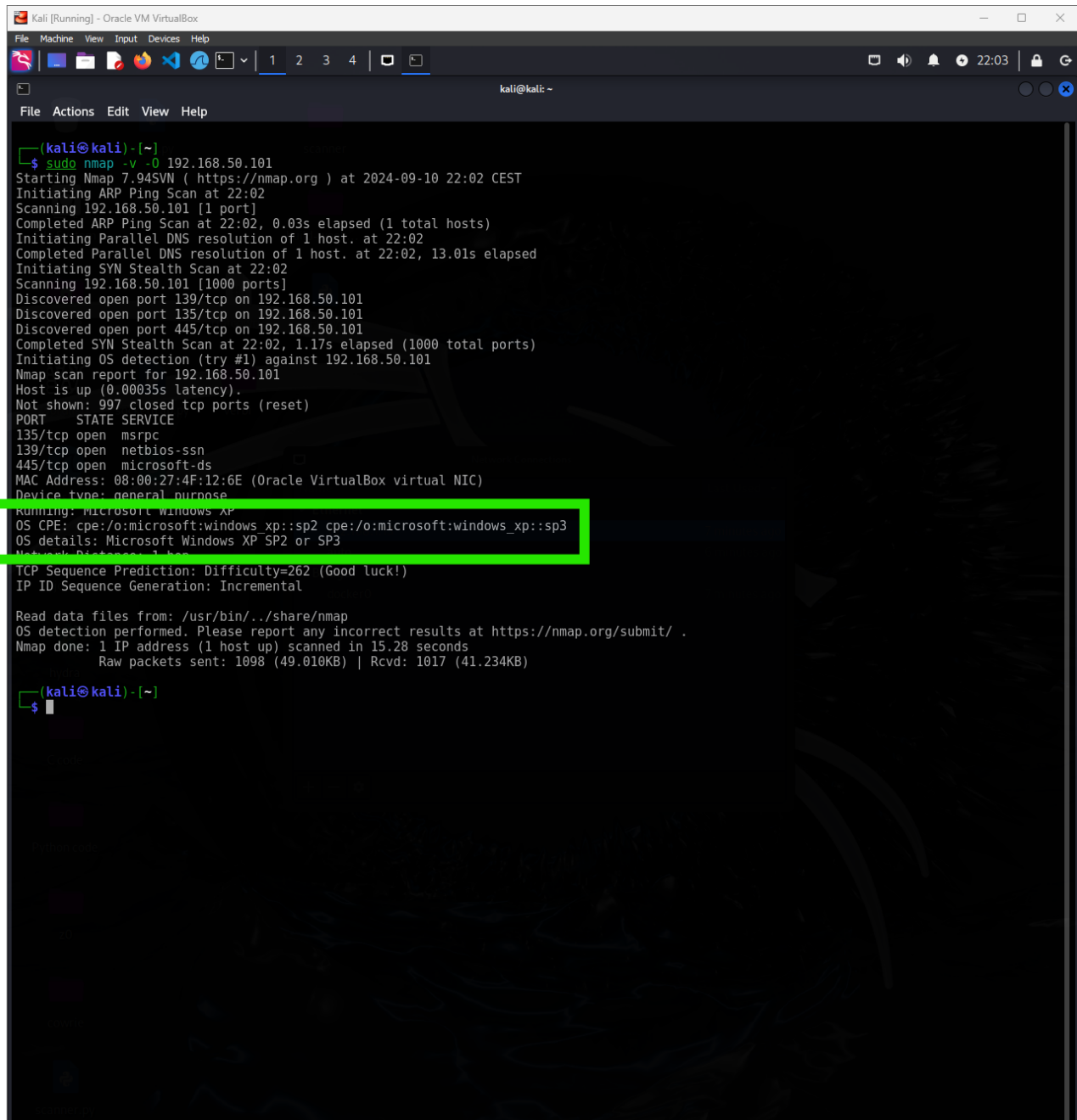
Starting Nmap 9.94SVN ( https://nmap.org ) at 2024-09-10 14:27 CEST
Nmap scan report for 192.168.2.101 (192.168.2.101)
Host is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:6D:40:00 (VirtualBox VM network interface)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.41 seconds

(kali@kali) - [~]
$
```

SERVIZI IN ASCOLTO CON LA LORO VERSIONE NEL **RIQUADRO BLU**.

Immettendo il comando `sudo nmap -O <IP TARGET WINDOWS XP>` sono risalito alla versione OS di quest' ultimo.



```
(kali@kali) - [~]
$ sudo nmap -v -O 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-10 22:02 CEST
Initiating ARP Ping Scan at 22:02
Scanning 192.168.50.101 [1 port]
Completed ARP Ping Scan at 22:02, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:02
Completed Parallel DNS resolution of 1 host. at 22:02, 13.01s elapsed
Initiating SYN Stealth Scan at 22:02
Scanning 192.168.50.101 [1000 ports]
Discovered open port 139/tcp on 192.168.50.101
Discovered open port 135/tcp on 192.168.50.101
Discovered open port 445/tcp on 192.168.50.101
Completed SYN Stealth Scan at 22:02, 1.17s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.50.101
Nmap scan report for 192.168.50.101
Host is up (0.00035s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:4F:12:6E (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.28 seconds
Raw packets sent: 1098 (49.010KB) | Rcvd: 1017 (41.234KB)

(kali@kali) - [~]
$
```

IP WINDOWS XP: 192.168.50.101 – IP KALI 192.168.50.100

```
File Actions Edit View Help

kali@kali: ~$ sudo nmap -sS -O -v 192.168.2.101
Starting Nmap ( https://nmap.org ) at 2024-09-10 14:21 CEST
Nmap scan report for 192.168.2.101 (192.168.2.101)
Host is up (0.046s latency).
Not shown: 655 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
33/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi
1524/tcp  open  bindshell
2049/tcp  open  nfs
2112/tcp  open  ftp
2380/tcp  open  mysql
3432/tcp  open  postgresql
5980/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  http
MAC Address: 88:98:27:6D:43:CD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.88 seconds

kali@kali: ~$ sudo nmap -sT -O -v 192.168.2.101
Starting Nmap ( https://nmap.org ) at 2024-09-10 14:21 CEST
Nmap scan report for 192.168.2.101 (192.168.2.101)
Host is up (0.046s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
33/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi
1524/tcp  open  bindshell
2049/tcp  open  nfs
2112/tcp  open  ftp
2380/tcp  open  mysql
3432/tcp  open  postgresql
5980/tcp  open  vnc
6080/tcp  open  x11
6667/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  http
MAC Address: 88:98:27:6D:43:CD (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.70 seconds

kali@kali: ~$
```

La differenza principale fra l'opzione **-sS** e **-sT** e' che l'opzione **TCP SYN scan (-sS)** a differenza del **TCP connect scan (-sT)** non attende la risposta ACK dalla destination generando un **RESET** e non completando la three-handshake-way e quindi meno rilevabile da un analisi essendo piu' "stealth". In oltre il metodo **-sS** ha bisogno di permessi di root a differenza di **-sT**.